Comments on IG Audit Questions
May 9, 2003

The FSA Security and Privacy Team reviewed the IG Audit Questions to compare them to the EDCAS C&A security requirements and test procedures. The IG Audit Questions are being considered for usage in the C&A process and therefore a review was necessary to identify and eliminate any overlaps. For each question in the IG Audit that was covered by EDCAS, a reference notation was made in the remarks section with the organization reference and the question in EDCAS. The process also lead to a number of comments that may assist the IG improve its questionnaire.

- There were a large number of duplicates throughout the questionnaire. The Team marked the duplicates and in the remarks section listed where they were duplicated previously in the document. Due to the excessively large amount of duplicates, the IG might want to revisit the documents and eliminate the overlaps from within the document. This will save time by avoiding repetitious questioning at testing time.
- There should be another column for answer response beyond Y and N; for yes and no. There needs to be a N/A (not applicable column). Many of these questions do not apply to Department of Education at this time. For example, questions about wireless and single sign on generally do apply to the Department. Currently, to respond to these questions, the system would have to answer no, which would imply that they are doing something wrong by not having these measures in place, when in reality, these measures are not even be applied.
- These questions need to be reorganized by topic. The same themes are revisited continuously in different sections of the document. It is confusing for a person reading the questions, which leads one to believe it would be difficult to administer the questions or more importantly to respond to vulnerability findings.
- The Department needs to reconsider using these questions for the C&A process. The C&A process is about testing requirements, specifically testing government requirements. The C&A process is not about testing best practices of unknown origin.. The IG questions have no clear link to Department of Education or federal government requirements and there is no clear mapping to the origin of the questions. Without clear traceability, it is difficult to consider the IG questions best practices. Some of the test questions, the “best practices,” also conflict with Ed policy (see page 21, question 11 F.)
  If ED decides to use the IG questions, perhaps they should be thought of as *security considerations* rather than security requirements. This would maintain the integrity of the C&A process.